

Privacy Impact Assessment Form

v 1.47.4

Status

Form Number

Form Date

Question

Answer

1 OPDIV:

2 PIA Unique Identifier:

2a Name:

3 The subject of this PIA is which of the following?

- General Support System (GSS)
 Major Application
 Minor Application (stand-alone)
 Minor Application (child)
 Electronic Information Collection
 Unknown

3a Identify the Enterprise Performance Lifecycle Phase of the system.

3b Is this a FISMA-Reportable system?

- Yes
 No

4 Does the system include a Website or online application available to and for the use of the general public?

- Yes
 No

5 Identify the operator.

- Agency
 Contractor

6 Point of Contact (POC):

POC Title POC Name POC Organization POC Email POC Phone

7 Is this a new or existing system?

- New
 Existing

8 Does the system have Security Authorization (SA)?

- Yes
 No

8b Planned Date of Security Authorization

 Not Applicable

<p>11 Describe the purpose of the system.</p>	<p>Traumatic Brain Injury Disparities in Rural Areas (TBIDRA) enables CDC to identify challenges that rural health care providers face in diagnosing and managing Traumatic Brain Injury (TBI) across the severity spectrum. It also facilitates the identification of innovative solutions to address gaps in services to improve clinical care and TBI outcomes in rural communities.</p>	
<p>12 Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)</p>	<p>TBIDRA collects and maintains survey data, names, e-mail addresses, mailing addresses, phone numbers, and demographic data from physicians, physician assistants, and nurse practitioners living in both rural and urban areas. No personal or health information will be collected or maintained. UserID, Pin and Password associated with respondents are used to identify the individual as a valid respondent to the contractor's survey instrument; all of which will be stored until the end of the contract. Users accessing the system do not require a user id/password; validation occurs via Active Directory.</p> <p>User access is not controlled via</p>	
<p>13 Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.</p>	<p>The Traumatic Brain Injury Disparities in Rural Areas (TBIDRA) is a system whose purpose is to collect data that will serve to aid CDC in identifying the challenges that rural health care providers face in diagnosing and managing TBI across the severity spectrum and beginning to identify innovative solutions to address gaps in services to improve clinical care and TBI outcomes in rural communities.</p> <p>The information system will collect and maintain survey data, names, e-mail address, mailing address, phone number, and demographic data from physicians, physician assistants, and nurse practitioners living in both rural and urban areas. No personal health information will be collected or maintained.</p> <p>The data will be collected orally via focus groups as well as through a one-time web survey. Information will be documented and saved on the Contractor's internal secured file server, as well as in the web server databases. A UserID, Pin & Password used to identify the individual as a valid respondent to the Contractor survey instrument. All this information will be stored temporarily until the end of the contract.</p>	
<p>14 Does the system collect, maintain, use or share PII?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>	

15 Indicate the type of PII that the system will collect or maintain.

<input type="checkbox"/> Social Security Number	<input type="checkbox"/> Date of Birth
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Photographic Identifiers
<input type="checkbox"/> Driver's License Number	<input type="checkbox"/> Biometric Identifiers
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Vehicle Identifiers
<input checked="" type="checkbox"/> E-Mail Address	<input checked="" type="checkbox"/> Mailing Address
<input checked="" type="checkbox"/> Phone Numbers	<input type="checkbox"/> Medical Records Number
<input type="checkbox"/> Medical Notes	<input type="checkbox"/> Financial Account Info
<input type="checkbox"/> Certificates	<input type="checkbox"/> Legal Documents
<input type="checkbox"/> Education Records	<input type="checkbox"/> Device Identifiers
<input type="checkbox"/> Military Status	<input type="checkbox"/> Employment Status
<input type="checkbox"/> Foreign Activities	<input type="checkbox"/> Passport Number
<input type="checkbox"/> Taxpayer ID	

Respondent user ID/Password

16 Indicate the categories of individuals about whom PII is collected, maintained or shared.

<input type="checkbox"/> Employees
<input checked="" type="checkbox"/> Public Citizens
<input type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies)
<input type="checkbox"/> Vendors/Suppliers/Contractors
<input type="checkbox"/> Patients
Other <input type="text"/>

17 How many individuals' PII is in the system?

18 For what primary purpose is the PII used?

19 Describe the secondary uses for which the PII will be used (e.g. testing, training or research)

20 Describe the function of the SSN.

20a Cite the **legal authority** to use the SSN.

21 Identify **legal authorities** governing information use and disclosure specific to the system and program.

22 Are records on the system retrieved by one or more PII data elements? Yes No

23 Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

- In-Person
- Hard Copy: Mail/Fax
- Email
- Online
- Other

Government Sources

- Within the OPDIV
- Other HHS OPDIV
- State/Local/Tribal
- Foreign
- Other Federal Entities
- Other

Non-Government Sources

- Members of the Public
- Commercial Data Broker
- Public Media/Internet
- Private Sector
- Other

23a Identify the OMB information collection approval number and expiration date.

The OMB information collection approval number is 0920-1218 and the expiration date 02/28/2021.

24 Is the PII shared with other organizations?

Yes

No

25 Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

A disclosure notification will be part of the script read to respondents on survey site to obtain consent (for web survey) and the process for focus groups and email communication to schedule participation.

26 Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Mandatory

27 Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Individuals can opt-out of the study. During the introductory script individuals will be advised that they can at any time opt-out of the study or refuse to answer any questions they do not wish to answer.

28 Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.

The Contractor contacts the participants via email and phone numbers on record to notify and obtain consent when major changes occur to the system.

29 Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.

Individuals with concerns about inappropriate attainment, use, or disclosure as well as inaccuracy of their PII may report their concerns to the Contractor's Institutional Review Board.

30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	Data collection will occur one-time. These methods will serve as the primary manner in which the data is reviewed for integrity, availability, accuracy, and relevancy.										
31	Identify who will have access to the PII in the system and the reason why they require access.	<table border="1"> <tr> <td data-bbox="732 237 951 296"><input type="checkbox"/> Users</td> <td data-bbox="959 237 1411 296"></td> </tr> <tr> <td data-bbox="732 296 951 363"><input checked="" type="checkbox"/> Administrators</td> <td data-bbox="959 296 1411 363"></td> </tr> <tr> <td data-bbox="732 363 951 430"><input type="checkbox"/> Developers</td> <td data-bbox="959 363 1411 430"></td> </tr> <tr> <td data-bbox="732 430 951 573"><input checked="" type="checkbox"/> Contractors</td> <td data-bbox="959 430 1411 573">To conduct interviews or manage the data collection process. Administrators (contractors) Administrators have full rights to</td> </tr> <tr> <td data-bbox="732 573 951 640"><input type="checkbox"/> Others</td> <td data-bbox="959 573 1411 640"></td> </tr> </table>	<input type="checkbox"/> Users		<input checked="" type="checkbox"/> Administrators		<input type="checkbox"/> Developers		<input checked="" type="checkbox"/> Contractors	To conduct interviews or manage the data collection process. Administrators (contractors) Administrators have full rights to	<input type="checkbox"/> Others	
<input type="checkbox"/> Users												
<input checked="" type="checkbox"/> Administrators												
<input type="checkbox"/> Developers												
<input checked="" type="checkbox"/> Contractors	To conduct interviews or manage the data collection process. Administrators (contractors) Administrators have full rights to											
<input type="checkbox"/> Others												
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	<p>Contractor uses the concept of role-based access control (RBAC) to give the appropriate permissions associated with each user role. RBAC uses the security principle of least privilege which gives the user the precise amount of privilege that is necessary to perform their job.</p> <p>Contractor administrators have full access to any files on the server once approval to gain access is granted.</p> <p>The developers do not require access to PII because they are needed to validate and test the application's functionality. The users do not require access to PII because they are there to give the survey to respondents and manage data collection.</p>										
33	Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	The least privilege model will be used to allow those with access to PII to be able to access the minimum amount of PII needed to perform their job. Users must request access to specific files needed and that is the only access they are permitted. No one will be granted more access than is necessary to perform their job.										
34	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	All personnel having system access are required to take Privacy and IT Security Awareness training upon hire and annually thereafter. This training has been reviewed and is compatible with CDC requirements to make them aware of their responsibilities for protecting the information being collected and maintained.										
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All system users are required to complete annual training requirements that consist of Ethics and Compliance training, security awareness course and sign the acknowledgment of the CDC Rules of Behavior which has been reviewed and is compatible with CDC requirements.										
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	<input checked="" type="radio"/> Yes <input type="radio"/> No										

<p>37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.</p>	<p>Records are retained and disposed of in accordance with the CDC Records Control Schedule (N1-442-09-1) and in accordance with contractual agreement. Record copy of study reports are maintained in agency from two to three years in accordance with retention schedules. Source documents for computer are disposed of when no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed.</p>	
<p>38 Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.</p>	<p>Administrative controls include a system security plan, contingency plan, regular back up of files and storage of backups off site, role-based security awareness training, least privilege access enforced through Active Directory groups, separate user and privileged accounts for administrators, policies and procedures in place for retention and destruction of PII, and a corporate incident response team and incident response plans.</p> <p>Technical controls include identification and authentication using unique user IDs, passwords, and smart cards, use of firewalls and intrusion detection/prevention systems, virus scanning software on all computers, and a security information and event management (SIEM) solution.</p> <p>Physical controls include guards, identification badges, key cards, and closed circuit TV.</p>	
<p>39 Identify the publicly-available URL:</p>	<p>This system is still in development and the publicly-available URL is not available yet.</p>	
<p>40 Does the website have a posted privacy notice?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>	
<p>40a Is the privacy policy available in a machine-readable format?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>	
<p>41 Does the website use web measurement and customization technology?</p>	<p><input type="radio"/> Yes <input checked="" type="radio"/> No</p>	
<p>42 Does the website have any information or pages directed at children under the age of thirteen?</p>	<p><input type="radio"/> Yes <input checked="" type="radio"/> No</p>	
<p>43 Does the website contain links to non- federal government websites external to HHS?</p>	<p><input type="radio"/> Yes <input checked="" type="radio"/> No</p>	
<p>General Comments</p>		

OPDIV Senior Official
for Privacy Signature